۱ .رمز مهم ترین ابزار حفظ امنیت کارت بانکی است که در نگهداری آن باید دقت بسیار زیادی شود و طبق الزامات امنیتی نباید به هیچ عنوان در اختیار فرد دیگری قرار گیرد؛ بر اساس قانون و الزامات شاپرک و بانک مرکزی، رمز کارت باید توسط خریدار در دستگاه کارتخوان وارد شود بر همین اساس همواره در خریدها رمز کارت بانکی را در دستگاه کارتخوان وارد کنید تا از کلاهبرداری با استفاده از اسکیمر و کپی شدن کارت بانکی دور بمانید؛ در صورتی که به اجبار کارت بانکی را به همراه رمز در اختیار دیگران قرار دادید و نسبت به فرد مشکوک بودید، فورا نسبت به تغییر رمز کارت بانکی اقدام کنید.

۲ .از انتخاب و قرار دادن رمزهای ساده و قابل حدس به خصوص سال تولد برای کارت بانکی در رمز اول و دوم خودداری کنید؛ همچنین یک رمز مشترک را برای تمامی کارت‌های بانکی انتخاب نکنید و رمزهایی متفاوت برای کارت‌های بانکی تعیین شود.

۳.رمز کارت بانکی را روی کارت بانکی یادداشت نکنید و در کنار کارت بانکی قرار ندهید چرا که علاوه بر کاهش امنیت، در صورت سرقت کارت احتمال برداشت غیرمجاز و سوءاستفاده از کارت بانکی بسیار زیاد است؛ همچنین از ارسال تصویر کارت بانکی در پیام رسان‌ها و شبکه‌های اجتماعی خودداری کنید.

۴.به صورت دوره ای (حداکثر سه ماه یکبار) رمز اول و دوم کارت بانکی خود را تغییر دهید تا از کلاهبرداری و سوءاستفاده دور باشید.

۵ .در صورت برخورداری بانک عامل خود از زیرساخت رمز اول و دوم یکبار مصرف نسبت به فعال سازی آن و استفاده از رمزهای پویا اقدام کنید تا تراکنش‌هایی امن‌تر داشته باشید تا در نهایت امکان سوءاستفاده کاهش پیدا کند.

۶.در هنگام افتتاح حساب و دریافت کارت بانکی نسبت به فعال سازی سیستم پیامکی بانک برای حساب خود اقدام نمایید تا در صورت برداشت و یا واریز وجه به حسابتان فوراً از موضوع مطلع شوید؛ برای فعال سازی پیامک حساب به یکی از شعب بانک عامل خود مراجعه کنید.

۷.برگ رسید ارائه شده از سوی دستگاه خودپرداز را در محل رها نکنید و در صورت نیاز نداشتن به رسید کاغذی آن را به صورت کامل از بین ببرید.

۸.یکی از ترفندهای رایج و خطرناک کلاهبرداران برای سرقت اطلاعات حساب بانکی و برداشت غیر مجاز مسابقات تلفنی و استفاده از دستگاه خودپرداز است که با عنوان کلاهبرداری با خودپرداز شناخته می‌شود؛ لازم است بدانید که لزومی ندارد در زمانی که پولی از طریق کارت بانکی به حساب شما منتقل خواهد شد به دستگاه خودپرداز مراجعه یا اقدامی کنید و تمامی درخواست‌های مراجعه به دستگاه خودپرداز به منظور واریز وجه در حساب شما کلاهبرداری است که باید به صورت فوری به پلیس فتا برای پیگیری بیشتر اطلاع داده شود.

۹ .فیشینگ یکی از روش‌های کلاهبرداری است که متاسفانه در طول سال‌های اخیر با افزایش روند خرید اینترنتی و استفاده از درگاه‌های پرداخت الکترونیک رشد بسیار زیادی داشته است؛ بر همین اساس رعایت ایمنی رمز دوم کارت بانکی و توجه به اصالت درگاه‌های پرداخت به منظور انجام تراکنش برای جلوگیری از افتادن در دام کلاهبرداران با ترفند فیشینگ و سرقت اطلاعات کارت بانکی نیاز است تا نکات امنیتی درگاه پرداخت را بررسی کنید که از جمله آنها باید به وجود قفل سبز در نوار آدرس اینترنت، وجود پروتکلHttps ، قرار گرفتن نام دامنه شاپرک به صورت مثال https://xxx.shaparak.ir و تغییر هر باره تصویر امنیتی و جایگاه اعداد در صفحه کلید مجازی اشاره داشت؛ همچنین توصیه می‌شود برای انجام تراکنش‌های اینترنتی از وای فای عمومی یا شبکه‌های اینترنتی که به امنیت آنها اعتماد ندارید استفاده نکنید تا احتمال سرقت اطلاعات کارت بانکی کاهش پیدا کند.

۱۰.از کارت بانکی خود کاملا محافظت کنید و در صورتی که دیگر به کارت بانکی نیاز ندارید، با مراجعه به شعبه بانک عامل نسبت به باطل و مسدودسازی کارت اقدام کنید، اما در صورتی که کارت را در محلی امن رها کرده‌اید، به هیچ عنوان رمز آن را به منظور جلوگیری از سوءاستفاده و پیشگیری از مشکلات قضایی ناشی از آن فاش نکنید.